PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-008619
(43)Date of publication of application : 12.01.1999

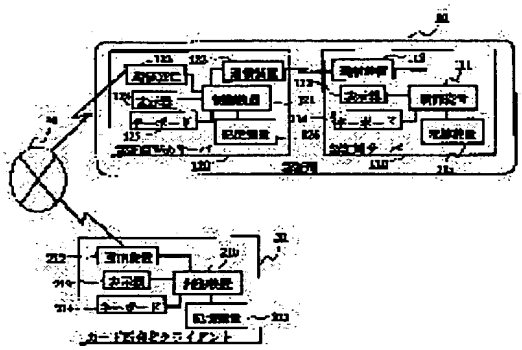
(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 9/08

(21)Application number : 09-160798
(22)Date of filing : 18.06.1997

(71)Applicant : HITACHI LTD
(72)Inventor : TOMIYAMA TOMOYA
CHIBA SANEYUKI
KAWATSURE YOSHIAKI
MATSUNAGA KAZUO
SUZAKI SEIICHI

(54) ELECTRONIC CERTIFICATE PUBLICATION METHOD AND SYSTEM THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To issue a certificate at a low cost and to enhance the security at the issue.
SOLUTION: In the electronic certificate publication method, an authentication station issues an electronic certificate via a network to a person to be authenticated who receives an issued certificate. The authentication station receives a document to be certificated in which a digital signature is made by using a key certificated by an electronic certificate and the name of the document to be certificated on request of issue from a client 20 based on the electronic certificate of a public key having already been issued by an authentication station 10 and on a public key of the person to be authenticated in the electronic certificate to authenticate whether or not the digital signature by the person to be authenticated is valid. When the digital signature is authenticated to be valid, the document is collated with a list containing electronic certrificates to be issued. In the case that the cetrificate requested by the authenticated person is able to be issued, the sent electronic cetrificate is authenticated, and when the authentication of the cetrificate is valid, the electronic cetrificate authenticating the public key of the authenticated person is issued.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平11－8619

(43)公開日　平成11年(1999)１月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｄ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｂ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｆ

審査請求　未請求　請求項の数５　ＯＬ　（全 16 頁）

(21)出願番号　特願平9－160798

(22)出願日　平成９年(1997)６月18日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　富山　朋哉
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内

(72)発明者　千葉　實之
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内

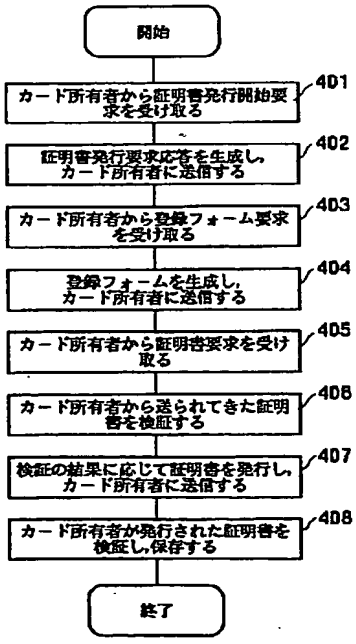
(74)代理人　弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　電子証明書発行方法及びシステム

(57)【要約】
【課題】　低コストで証明書を発行することとその発行の際のセキュリティ強度を高めること。
【解決手段】　証明書を発行してもらう被認証者に対して認証局がネットワークを介して電子証明書を発行する電子証明書発行方法であって、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対して、前記電子証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書名の入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、前記電子証明書で発行可能な証明書のリストと照合し、前記被認証者が要求した証明書が発行可能である場合には、送信された電子証明書の検証を行い、検証できた場合に、前記被認証者の公開鍵を認証した電子証明書を発行する。

図4



【特許請求の範囲】
【請求項１】　証明書を発行してもらう被認証者に対して認証局がネットワークを介して電子証明書を発行する電子証明書発行方法であって、
ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対して、前記電子証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書名の入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、前記電子証明書で発行可能な証明書のリストと照合し、前記被認証者が要求した証明書が発行可能である場合には、送信された電子証明書の検証を行い、検証できた場合に、前記被認証者の公開鍵を認証した電子証明書を発行することを特徴とする証明書発行方法。
【請求項２】　前記請求項１に記載の電子証明書発行方法であって、
前記ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵と発行を要求する証明書名と共に予め認証局に登録してある被認証者を特定する確認情報を前記電子証明書で証明済の鍵でデジタル署名を施したものの入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できた後に、前記被認証者の確認情報の検証を行い、検証できたときに前記電子証明書で発行可能な証明書のリストと照合することを特徴とする証明書発行方法。
【請求項３】　電子証明書を発行してもらう被認証者のクライアントと、前記被認証者に電子証明書を発行する認証局のサーバとがネットワークを介して接続されてなる電子証明書発行システムであって、
前記被認証者のクライアントは、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対し、前記電子証明書で証明済の鍵でデジタル署名し、前記認証局のサーバに送信して他の電子証明書の発行要求を行う発行要求手段と、前記認証局から送信されてきた電子証明書を保存する手段とを備え、
前記認証局のサーバは、各電子証明書から発行可能な他の電子証明書群をまとめた発行可能証明書リストと、前記被認証者のデジタル署名が妥当であるか否かを検証する署名検証手段と、前記署名検証手段により、署名が妥当であると検証できたときに、送信されてきた送信電子証明書と発行可能証明書リストと照合する証明書照合手段と、前記証明書照合手段により、前記被認証者が要求した要求電子証明書が発行可能であるとき、前記被認証者からの送信電子証明書の検証を行う電子証明書検証手段と、前記電子証明書検証手段により、前記送信電子証明書が検証されたとき、前記被認証者の公開鍵を認証した要求電子証明書を発行する手段とを備えたことを特徴とする電子証明書発行システム。
【請求項４】　前記請求項３に記載の電子証明書発行システムにおいて、
前記被認証者のクライアントの発行要求手段は、予め認証局に登録してある被認証者を特定する確認情報を前記電子証明書で証明済の鍵でデジタル署名したものを送信する手段を備え、
前記認証局のサーバは、前記被認証者の確認情報の検証を行う確認情報検証手段を備えたことを特徴とする電子証明書発行システム。
【請求項５】　前記請求項３、または４に記載の電子証明書発行システムにおいて、
前記認証局のサーバは、前記発行可能証明書リストを基に、送信電子証明書で発行可能な他の電子証明書のリスト、または前記要求電子証明書の発行に必要となる電子証明書を前記被認証者のクライアントに送信する手段を備えたことを特徴とする電子証明書発行システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、公開鍵暗号方式を用いたオープンなネットワーク上で行われる電子証明書発行およびシステムに関し、特に低コストで証明書を発行できる電子証明書発行方法およびシステムに適用して有効な技術に関するものである。
【０００２】
【従来の技術】近年では、インターネットなどオープンなネットワーク上で電子商取引が行われているが、インターネットを用いて電子商取引を行う場合には個人情報等のデータのやり取りの安全性が問題となっている。
【０００３】つまり、データの漏洩や、改竄、配送元のなりすまし等の犯罪を比較的容易に行うことができるからである。
【０００４】このような問題に対して、従来では、共通鍵暗号方式や、公開鍵暗号方式といった暗号化方式を使って、安全なデータのやり取りが実現されている。
【０００５】ここで、共通鍵暗号方式とは、暗号化する時に使用する鍵と復号化する時に使用する鍵が同じである暗号方式であり、暗・復号速度が高速なので、大量のデータを暗号化するのに適している。
【０００６】これに対して公開鍵暗号方式とは、他者に見せない鍵（秘密鍵）と、それに対応する、他者に公開する鍵（公開鍵）とのペアからなり、一方の鍵を使用して作られた暗号文は、ペアのもう一方の鍵を使用しなければ復号化できない方式であり、また、一方の鍵からもう片方の鍵を類推することは困難であるという性質をもっており、不特定多数の人と通信することに適している。
【０００７】また、これらの他にも認証局という、信頼できる第３者機関が発行した電子証明書（以下、証明書と記す）を使用することにより、通信相手の身元を証明し、通信元のなりすましを防止する方法が提案されてい

る。

【０００８】この認証局が証明書を発行する手順は、次の通りである。

【０００９】まず、被認証者が認証局に対して発行要求メッセージを送り、認証局から認証局の証明書を入手する。認証局の証明書を受理した被認証者は、証明書を検証する。その証明書が、上位認証局により発行されていた場合、その上位認証局の証明書を入手することを繰り返す。最終的に信用できる最上位の認証局の証明書を検証することにより判断する。検証できたときは、認証局に対して、発行の申請を行う証明書の種類がわかるような情報および登録フォーム要求メッセージを送る。ここで、登録フォームとは、証明書発行に必要な事柄を記入するフォームである。

【００１０】このメッセージを受理した認証局は、証明書の種類を確定しその証明書発行に必要な項目を記入する登録フォームにデジタル署名をつけて被認証者に送る。

【００１１】ここで、デジタル署名とは、具体的には、署名したいメッセージをハッシュ関数とよばれる特殊な関数を用いて、一定の長さのハッシュ値とよばれる値に変換したものを作成し、そのハッシュ値に対してメッセージ作成者の秘密鍵で暗号化することである。ハッシュ値は一意に定まるため、受け取ったメッセージのハッシュと、受け取ったデジタル署名を公開鍵で復号化したものが一致するかどうかを確認することにより、メッセージの改竄を確認することができる。

【００１２】デジタル署名つき登録フォームを受け取った被認証者は、署名を確認し、確認できたとき、被認証者の登録鍵、すなわち公開鍵と秘密鍵を生成し、公開鍵と登録者本人であることの根拠となる個人情報、たとえば口座番号とを暗号化して認証局に送る。

【００１３】認証局は、送られてきたメッセージを復号化して、登録者本人であることの根拠となる個人情報を、その情報に関する機関に問い合わせることによって確認する。例えば、個人情報として口座番号を用いた場合は、銀行に問い合わせることになる。問い合わせた結果、情報が正しいならば、被認証者の公開鍵の証明書を作成し、この証明書を被認証者へ送る。

【００１４】以上のような手順は、例えば、SET(Secure Electronic Transaction Specification ,Draft for testing, June 17,1996, MasterCard, VISA)で用いられている。

【００１５】

【発明が解決しようとする課題】本発明者は、上記従来技術を検討した結果、以下の問題点を見いだした。

【００１６】証明書発行の際に登録者本人であることを確認する従来の方法は、被認証者から認証局へ口座番号を送り、認証局がその口座番号が正しいかどうかを銀行に確認することによって行われている。

【００１７】この方法では、証明書発行の際に口座番号の確認を認証局とは別の機関（銀行）に依頼しているため、コストが大きくなるという問題点がある。

【００１８】また、暗号化されているとはいえ、証明書とは直接関係のない個人情報が、オープンなネットワーク上を通過するという問題点もある。

【００１９】本発明の目的は、被認証者が既に取得している証明書を本人認証の根拠とすることにより、本人認証のコストを下げ、証明書発行にかかるコストを下げることが可能な技術を提供することにある。

【００２０】本発明の他の目的は、証明書発行依頼の際に、既に発行されている証明書を基に個人情報（例えば、口座番号）というプライバシーおよびセキュリティ上に問題のある情報を送信せずに済ませることにより、全体のセキュリティ強度を高めることが可能な技術を提供することにある。

【００２１】本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかになるであろう。

【００２２】

【課題を解決するための手段】本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

【００２３】証明書を発行してもらう被認証者に対して認証局がネットワークを介して電子証明書を発行する電子証明書発行方法であって、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対して、前記電子証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書名の入力を受け、前記被認証者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、前記電子証明書で発行可能な証明書のリストと照合し、前記被認証者が要求した証明書が発行可能である場合には、送信された電子証明書の検証を行い、検証できた場合に、前記被認証者の公開鍵を認証した電子証明書を発行する。

【００２４】また、電子証明書を発行してもらう被認証者のクライアントと、前記被認証者に電子証明書を発行する認証局のサーバとがネットワークを介して接続されてなる電子証明書発行システムであって、前記被認証者のクライアントは、ある認証局が既に発行した公開鍵の電子証明書とその電子証明書における被認証者の公開鍵に対し、前記電子証明書で証明済の鍵でデジタル署名し、前記認証局のサーバに送信して他の電子証明書の発行要求を行う発行要求手段と、前記認証局から送信されてきた電子証明書を保存する手段とを備え、前記認証局のサーバは、各電子証明書から発行可能な他の電子証明書群をまとめた発行可能証明書リストと、前記被認証者のデジタル署名が妥当であるか否かを検証する署名検証手段と、前記署名検証手段により、署名が妥当であると検証できたときに、送信されてきた送信電子証明書と発

行可能証明書リストと照合する証明書照合手段と、前記証明書照合手段により、前記被認証者が要求した要求電子証明書が発行可能であるとき、前記被認証者からの送信電子証明書の検証を行う電子証明書検証手段と、前記電子証明書検証手段により、前記送信電子証明書が検証されたとき、前記被認証者の公開鍵を認証した要求電子証明書を発行する手段とを備える。

【００２５】

【発明の実施の形態】以下、本発明の実施の形態を図面を用いて説明する。

【００２６】図１は、本発明の一実施形態にかかる証明書発行システムの構成を示すブロック図である。本実施形態では、既に取得してあるクレジットカードを基に新たな電子証明書を取得する場合を例に取り挙げて説明していく。

【００２７】本実施形態の証明書発行システムは、図１に示すように、電子証明書（以下、証明書と略す）を発行する認証局１０と、証明書発行を依頼する被認証者（以下、カード所有者と記す）のクライアント２０と、電子商取引を行うネットワークであるインターネット３０とから構成される。

【００２８】上述した認証局１０は、実際の処理を行う認証局サーバ１１０と、カード所有者のクライアント２０からインタネット３０経由で入力を受け付け、認証局サーバ１１０へ中継し、その結果を認証局サーバ１１０からカード所有者のクライアント２０へ送信する認証局Ｗｅｂサーバ１２０とから構成される。

【００２９】認証局サーバ１１０は、認証局Ｗｅｂサーバ１２０と通信を行う通信装置１１２と、表示器１１３と、キーボード１１４と、証明書データベース、証明書名データベース、認証局の署名鍵および交換鍵が格納される記憶装置１１５と、これら全てを制御する制御装置１１１とからなる。

【００３０】認証局Ｗｅｂサーバ１２０は、認証局サーバ１１０と通信を行う通信装置１２２と、インターネットに接続される通信装置１２３と、表示器１２４と、キーボード１２５と、Ｗｅｂサーバソフトウエアが格納される記憶装置１２６と、これら全てを制御する制御装置１２１とからなる。

【００３１】カード所有者のクライアント２０では、証明書データベースやカードホルダの署名鍵、共通鍵などを格納する記憶装置２１１と、インターネットに接続する通信装置２１２と、表示器２１３と、キーボード２１４と、これら全てを制御する制御装置２１０とからなる。

【００３２】図２は、認証局１０の構成を詳細に説明するための図である。

【００３３】図２に示すように、認証局１０の認証局サーバ１１０の記憶装置１１５には、証明書データベース１１５４０と証明書名データベース１１５３０、署名鍵公開鍵PBCPSG（１１５１１）と署名鍵個人鍵PVCPSG（１１５１２）とその証明書１１５１３とからなる認証局の署名鍵１１５１０、鍵交換鍵公開鍵PBCPEX（１１５２１）と鍵交換鍵個人鍵PVCPEX（１１５２２）とその証明書１１５２３とからなる鍵交換鍵１１５２０が保存されている。

【００３４】この証明書データベース１１５４０は、公開鍵１１５４３と、その公開鍵の対象（持ち主）１１５４２、証明書１１５４１をレコードとするデータベースであり、証明書名データベース１１５３０は、証明書名１１５３２と、その証明書を発行するのに必要となる条件である証明書名組１１５３３と、その証明書を使用するブランド１１５３１をレコードとするデータベースである。

【００３５】制御装置１１１は、通信装置１１２を通じて認証局Ｗｅｂサーバ１２０に接続され、必要に応じて証明書データベース１１５４０に格納されている証明書１１５４１、および証明書名データベース１１５３０に格納されている証明書名組１１５３３、認証局１０の署名鍵公開鍵１１５１１および署名鍵個人鍵１１５１２を認証局Ｗｅｂサーバ１２０へ送信する。

【００３６】認証局Ｗｅｂサーバ１２０の制御装置１２１は、認証局Ｗｅｂサーバ１２０のＷｅｂサーバソフトウエア１２６１０を記憶装置１２６からロードし、実行する。

【００３７】Ｗｅｂサーバソフトウエア１２６１０は、http（Hypertext Transport Protocol）に基づいて通信を行うプログラムである。

【００３８】図３は、カード所有者のクライアント２０を詳細に説明するための図である。

【００３９】カード所有者２０のクライアントの記憶装置２１１には、Ｗｅｂブラウザソフトウエア２１１１０と、署名鍵秘密鍵２１１６０と、証明書データベース２１１４０と、カード所有者２０の署名鍵公開鍵PBCHSG'（２１１２０）および署名鍵個人鍵PVCHSG'（２１１３０）と、それぞれの共通鍵＃１～＃３（２１１７１～２１１７３）と、署名鍵公開鍵リスト２１１８０とが保存される。

【００４０】証明書データベース２１１５０は、署名鍵公開鍵名２１１５３、その証明書が使える相手（ブランド名）２１１５２、証明書２１１５１をレコードとするデータベースである。

【００４１】次に、図４を用いて本実施形態の証明書発行システムの各制御装置における証明書発行処理の概要の説明を行い、その後、各ステップの詳細をそれぞれの図を用いて説明する。

【００４２】カード所有者が、Ｗｅｂブラウザソフトウエア２１１１０を通じて、認証局１０に対して、証明書発行を依頼する（ステップ４０１）。

【００４３】認証局１０は、カード所有者のクライアン

ト２０から証明書発行依頼を受け取ると、証明書発行要求応答を生成してカード所有者のクライアント２０に送信する。このとき、カード所有者へ認証局の公開鍵を送付する（ステップ４０２）。

【００４４】カード所有者は、認証局１０から証明書発行要求応答を受け取り、認証局１０の証明書の検証を行い、登録フォーム要求を認証局１０へ送信する（ステップ４０３）。

【００４５】認証局１０は、カード所有者のクライアント２０から登録フォーム要求を受け取ると、登録フォームを生成し、カード所有者のクライアント２０に送信する（ステップ４０４）。

【００４６】カード所有者は、登録フォームに必要事項を記入し、証明書要求を認証局１０へ送付する。このとき、カード所有者は、カード所有者の公開鍵を送付する（ステップ４０５）。

【００４７】認証局１０は、カード所有者のクライアント２０から送られてきた登録フォームに含まれている証明書を検証する（ステップ４０６）。

【００４８】認証局１０は、ステップ４０６の検証結果に応じて、証明書を発行し、カード所有者のクライアント２０に送付する（ステップ４０７）。

【００４９】カード所有者のクライアント２０では、発行された証明書を検証し、保存する（ステップ４０８）。

【００５０】上述したステップ４０２の詳細を図５を用いて説明する。

【００５１】ステップ４０２は、まず、認証局サーバ１１０が、証明書発行申請メッセージに対する応答メッセージを生成し、署名する（ステップ５０１）。

【００５２】認証局１０は、認証局１０の鍵交換鍵及び署名鍵のそれぞれの公開鍵PBCPEX（１１５２１）、PBCPSG（１１５１１）と、それぞれの証明書CertPBCPEX（１１５２３）、CertPBCPSG（１１５１３）と、ステップ５０１で作成した署名つき応答メッセージを、カード所有者のクライアント２０に送信する(ステップ５０２)。

【００５３】次に、上述したステップ４０３を図６を用いて詳細に説明する。

【００５４】ステップ４０３は、まず、カード所有者のクライアント２０が、証明書CertPBCPEX（１１５２３）、CertPBCPSG（１１５１３）の妥当性を、SET(Secure Electronic Transaction Specification, Draftfor testing, June 17, 1996, MasterCard, VISA, BookII, PartII Certificate Management, Ch.1, Sec.3, Certificate Chain Validation) と同様に検証する（ステップ６０１）。この妥当性の検証は、例えば、証明書が有効期限内であるか否かのチェック等である。

【００５５】検証の結果、妥当でなければ処理を中断し、妥当であれば処理を続ける（ステップ６０２）。

【００５６】カード所有者は、キーボード２１４を通じて登録フォーム選択情報を取り込む（ステップ６０３）。ここで、登録フォーム選択情報とは、消費者が発行してもらいたい証明書を選択するために必要な情報である。例えば、その証明書が利用できるカード会社名（ブランド名）などである。

【００５７】カード所有者のクライアント２０は、登録フォーム要求メッセージおよび共通鍵（＃１）SymK＃１を作成する（ステップ６０４）。

【００５８】カード所有者のクライアント２０は、登録フォーム要求メッセージを共通鍵SymK ＃１で暗号化し、また、登録フォーム選択情報と共通鍵SymK ＃１を認証局の鍵交換鍵公開鍵PBCPEX（１１５２１）で暗号化する（ステップ６０５）。

【００５９】カード所有者２０は、ステップ６０５で作成したメッセージを認証局１０へ送信する（ステップ６０６）。

【００６０】次に、上述したステップ４０４を図７を用いて詳細に説明する。

【００６１】ステップ４０４は、まず、認証局１０が、認証局１０の鍵交換鍵個人鍵PVCPEX１（１５２２）で、登録フォーム選択情報と共通鍵SymK ＃１を復号化し（ステップ７０１）、続いて、共通鍵SymK＃１で登録フォーム要求を復号化し（ステップ７０２）、登録フォーム選択情報から証明書発行に必要な証明書名組を決定し、登録フォームを作成する（ステップ７０３）。この証明書名組の決定の方法としては、例えば、

（１）登録フォーム選択情報に記述されているブランド名をキーにして、認証局の証明書名データベースから検索する

（２）登録フォーム選択情報にブランド名だけでなく、必要な証明書名組まで含めておく

などがある。

【００６２】そして、認証局１０は、ステップ７０３で作成した登録フォームに対して、認証局１０の署名鍵個人鍵PVCPSG（１１５１２）で署名し（ステップ７０４）、ステップ７０４で作成した署名つき登録フォームに、認証局１０の証明書CertPBCPSG（１１５１３）をつけ、カード所有者のクライアント２０へ送信する（ステップ７０５）。このように、前記証明書名データベースを基に、送信電子証明書で発行可能な他の証明書のリスト、または証明書の発行に必要となる証明書組をカード所有者のクライアントに送信することにより、証明書発行にかかる手間を少なくすることができる。

【００６３】次に、上述したステップ４０５を図８を用いて詳細に説明する。

【００６４】ステップ４０５は、図８に示すように、まず、カード所有者のクライアント２０が、受信した署名の証明書CertPBCPSGの妥当性を、SETと同様な手段により検証する（ステップ８０１）。

【００６５】その検証の結果、妥当でなければ処理を中

断し、妥当であれば処理を続け（ステップ８０２）、カード所有者の署名鍵公開鍵PBCHSG'（２１１２０）および秘密鍵PVCHSG'（２１１６０）を生成し、記憶装置２１１に保存し（ステップ８０３）、受信した登録フォームに必要事項を記入してこれを登録事項とする（ステップ８０４）。

【００６６】その後、カード所有者のクライアント２０は、受信した証明書名組にしたがって、証明書データベース２１１４０から証明書を検索し、証明書組を作成する（ステップ８０５）。

【００６７】ここで、証明書組とは、１個以上の複数個の証明書を、例えばリスト構造のように、ひとつのまとまりにしたものである。

【００６８】カード所有者は、その証明書組を構成している複数個の証明書からカード所有者の署名鍵公開鍵２１１２０を取り出し、カード所有者署名鍵公開鍵リストPBCHSGL（２１１８０）とする（ステップ８０６）。

【００６９】その後、カード所有者のクライアント２０は、共通鍵SymK ＃２（２１１７２）、共通鍵SymK ＃３（２１１７３）を生成して記憶装置２１１に保存し（ステップ８０７）、登録事項を含んだ証明書要求メッセージを作成する（ステップ８０８）。

【００７０】カード所有者２０は、証明書要求メッセージおよびカード所有者の署名鍵公開鍵PBCHSG'（２１１２０）、共通鍵SymK ＃２（２１１７２）に対して、カード所有者の署名鍵公開鍵PBCHSG"" で署名をつける（ステップ８０９）。ここで、PBCHSG"" はカード所有者署名鍵公開鍵リストPBCHSGL（２１１８０）に含まれているいずれか１個の公開鍵である。このPBCHSG""の選び方は、例えば、PBCHSGLの先頭の公開鍵を選択するとよい。このステップ８０９で、PBCHSG""の代わりにPBCHSGを使用すると、不正な証明書を使用することができるため、PBCHSG"" を使用することが必須である。なお、既存のSETでは、本人確認を口座番号などを利用して行っているためPBCHSGを使用しても構わない。登録する公開鍵PBCHSG' は、PBCHSG"" と同一とすることもできる。

【００７１】カード所有者のクライアント２０は、ステップ８０９の結果を、共通鍵SymK＃３（２１１７３）で暗号化し（ステップ８１０）、続いて、証明書組と共通鍵SymK ＃３（２１１７３）を、認証局の鍵交換鍵公開鍵PBCPEX（１１５２１）で暗号化し（ステップ８１１）、ステップ８１０およびステップ８１１で作成したものを、認証局１０へ送信する（ステップ８１２）。

【００７２】次に、上述したステップ４０６を図９を用いて詳細に説明する。

【００７３】ステップ４０６は、図９に示すように、まず、認証局１０が、カード所有者のクライアント２０から受信したメッセージに対して、認証局の鍵交換鍵個人鍵PVCPEX（１１５２２）を使って、証明書組と共通鍵SymK ＃３（２１１７３）を復号化する（ステップ９０１）。

【００７４】その後、認証局１０は、図８に示したステップ８１０で暗号化された部分を共通鍵SymK ＃３（２１１７３）で復号化し（ステップ９０２）、カード所有者の署名をカード所有者の署名鍵公開鍵PBCHSG""を使って検証し（ステップ９０３）、検証の結果、妥当でなければ処理を中断し、妥当であれば処理を続行する（ステップ９０４）。

【００７５】次に、上述したステップ４０８を図１０を用いて詳細に説明する。

【００７６】ステップ４０７は、図１０に示すように、まず、認証局１０が、証明書組を分解し（ステップ１００１）、各々の証明書を検証し、証明書値を計算する（ステップ１００２）。

【００７７】その後、認証局１０は、証明書要求メッセージから発行する証明書の名前を取り出し、証明書名データベース１１５３０からその証明書を発行するために必要な証明書名組１１５３３を検索し（ステップ１００３）、ステップ１００１の証明書名組１１５３３にステップ１００２の証明書値を代入して、証明書組値を計算する（ステップ１００４）。ここでの証明書値は、証明書が妥当であれば" t" 、妥当でなければ" f" と言う値を取る。また、証明書名組とは、複数の証明書名CN1,...CNnを論理演算子(∧、∨、¬)で結合したものである。

【００７８】例えば、(C1∧C2)∨(¬C3) は、証明書名組であり、その証明書名組の値とは、それぞれの証明書の値を証明書名組の「証明書名」へ代入し、論理演算した結果の値である。計算（論理演算）には、以下の論理規則を用いる。

【００７９】A, B, C は、0 個以上のt, fを∧, ∨, ¬で結合した式を表す。結合度は、¬, ∧, ∨の順で弱くなる。

【００８０】(1) t ∧t →t
(2) t ∧f →f
(3) f ∧t →f
(4) f ∧f →f
(5) t ∨t →t
(6) t ∨f →t
(7) f ∨t →t
(8) f ∨f →f
(9) ¬t →f
(10) ¬f →t
(11) A ∧B ∧C →(A ∧B) ∧C
(12) A ∨B ∨C →(A ∨B) ∨C

その後、認証局１０は、その他の条件を確認する。ここで、「その他の条件」とは、証明書の妥当性以外の条件であり、例えば、「ある友の会の会員である」、「年齢が35歳以上である」などのカード所有者本人を確認する

ものである。これらの条件を、認証局１０は、オンラインあるいはオフラインで確認し、その結果、条件に合っていれば条件値を”ｔ”　とし、条件に合わなければ条件値を”ｆ”　とする（ステップ１００５）。これにより、より確実に証明書の検証を行うことが可能になる。

【００８１】その後、認証局１０は、ステップ１００４、ステップ１００５の結果、証明書組値Ａ条件値を前述の論理規則にしたがって計算し、その結果が”ｆ”であれば処理を中断し、その結果が”ｔ”であれば処理を続行する（ステップ１００６）。

【００８２】そして、証明書組値が”ｔ”の場合、認証局１０は、カード所有者に対して、請求されていた証明書を発行するため、カード所有者の署名鍵公開鍵PBCHSG'（２１１２０）に対して認証局１０が署名した証明書CertPBCHSG'（２１１４０）を作成し（ステップ１００７）、証明書要求応答メッセージを作成、署名して、共通鍵SymK ＃２（２１１７２）で暗号化し（ステップ１００８）、証明書CertPBCHSG'（２１１４０）、および、ステップ１００８で作成した署名つき証明書要求応答メッセージを暗号化したものと、認証局１０の証明書CertPBCPSG（１１５１３）とを、カード所有者２０に対して送信する（ステップ１００９）。

【００８３】次に、上述したステップ４０９を図１１を用いて詳細に説明する。

【００８４】ステップ４０９は、図１１に示すように、まず、カード所有者のクライアント２０が、認証局から受信した証明書CertPBCPSG（２１１１３）の妥当性を、上述したように、SETと同様に検証する（ステップ１１０１）。

【００８５】その検証の結果、妥当でなければ処理を中断し、妥当であれば処理を続け（ステップ１１０２）、共通鍵Sym ＃２（２１１７２）を記憶装置２１１から取り出し、この共通鍵Sym ＃２（２１１７２）で証明書応答メッセージを復号化し（ステップ１１０３）、認証局１０の署名鍵公開鍵PBCPSG（１１５１１）で署名を検証し（ステップ１１０４）、署名が確認されなければ処理を中断し、確認されれば処理を続行する（ステップ１１０５）。

【００８６】そして、カード所有者のクライアント２０は、発行された証明書CertPBCHSG'（２１１４０）を記憶装置２１１に保存する（ステップ１１０６）。

【００８７】したがって、説明してきたように、ある認証局が既に発行した公開鍵の証明書とその証明書におけるカード所有者の公開鍵に対して、証明書で証明済の鍵でデジタル署名を施したものと発行を要求する証明書名の入力を受け、カード所有者のデジタル署名が妥当であるか否かを検証し、妥当であると検証できたときは、証明書と証明書名データベースとを照合し、カード所有者が要求した証明書が発行可能である場合には、送信された証明書の検証を行い、検証できた場合に、カード所有者の公開鍵を認証した証明書を発行することにより、カード所有者の身元確認の根拠として、電子的に送付可能で信頼性のある既に取得した証明書を用いることが可能になり、カード所有者から認証局へ口座番号を送ったり、認証局がその口座番号が正しいかどうかを銀行に確認したりする必要がなくなるので、低コストで証明書を発行することが可能になる。

【００８８】また、プライバシーに関わる個人情報を送付する必要がなくなるため、全体のセキュリティ強度を高めることが可能になる。

【００８９】なお、上述した証明書発行処理を行う証明書発行システムの各制御装置は、コンピュータで実行可能なプログラムで実現される場合もあり、そのときのプログラムは、フロッピーディスク、ＣＤ・ＲＯＭ、マスクＲＯＭ等の記憶媒体で一般ユーザに提供される。この場合、さらに、これら処理の他にＧＵＩプログラム等の他のプログラムと組み合わせてユーザに提供することもある。

【００９０】また、上述した記憶媒体で提供する代替手段として、インタネット等のネットワークを通じて有償で提供することもある。

【００９１】以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【００９２】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記のとおりである。

【００９３】カード所有者の身元確認の根拠として、電子的に送付可能で信頼性のある既取得証明書を用いることが可能になり、カード所有者から認証局へ口座番号を送ったり、認証局がその口座番号が正しいかどうかを銀行に確認したりする必要がなくなるので、低コストで証明書を発行することが可能になる。

【００９４】また、プライバシーに関わる個人情報を送付する必要がなくなるため、全体のセキュリティ強度を高めることが可能になる。

【図面の簡単な説明】

【図１】本発明の実施形態にかかる電子証明書発行システムの構成を説明するためのブロック図である。

【図２】認証局の構成を詳細に説明するための図である。

【図３】カード所有者のクライアントを詳細に説明するための図である。

【図４】本実施形態の証明書発行システムの各制御装置における証明書発行処理の概要を説明するためのフローチャートである。

【図５】認証局が、カード所有者からの証明書要求メッ

セージに応答するメッセージを作成し、カード所有者へ送信する処理を示すフローチャートである。

【図６】カード所有者が、認証局から証明書要求応答メッセージを受け取って、認証局へ登録フォーム要求メッセージを送信する処理を示すフローチャートである。

【図７】認証局が登録フォームを生成し、カード所有者に送信する処理を示すフローチャートである。

【図８】カード所有者が登録フォームを記入し、証明書要求を認証局へ送信する処理を示すフローチャートである。

【図９】認証局がカード所有者の証明書組を検証する処理を示すフローチャートである。

【図１０】認証局が、検証の結果に応じて証明書を発行し、カード所有者へ証明書を送信する処理を示すフローチャートである。

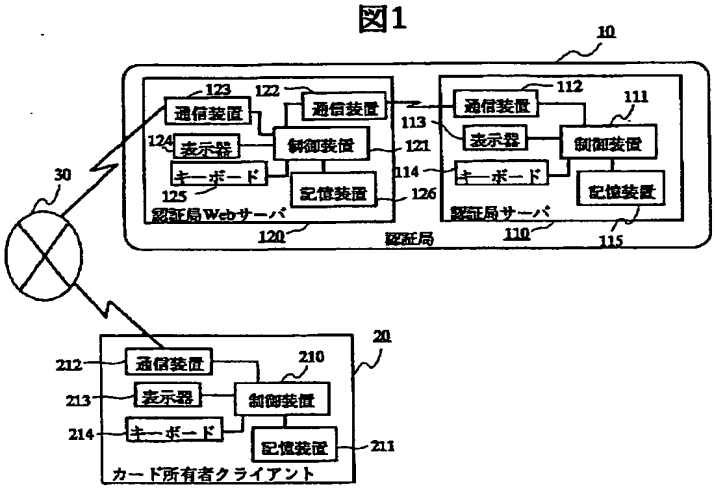
【図１１】カード所有者が、認証局によって発行された証明書を検証し保存する処理を示すフローチャートである。

【符号の説明】

１０…認証局、２０…クライアント、３０…インターネット、１１０…認証局サーバ、１１１…制御装置、１１２…通信装置、１１３…表示器、１１４…キーボード、１１５…記憶装置、１２０…認証局Ｗｅｂサーバ、１２１…制御装置、１２２…通信装置、１２３…通信装置、１２４…表示器、１２５…キーボード、１２６…記憶装置、２１０…制御装置、２１１…記憶装置、２１２…通信装置、２１３…表示器、２１４…キーボード。

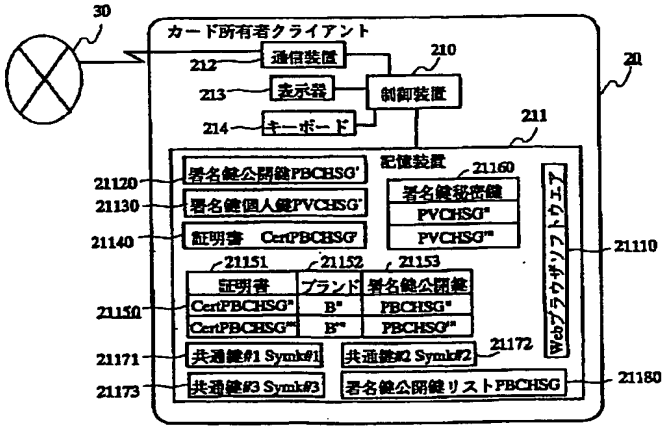
【図１】

図1



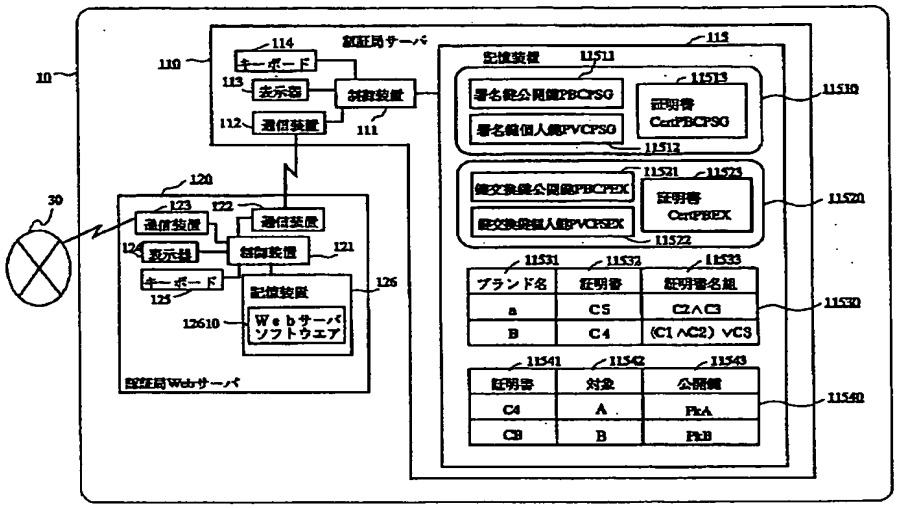
【図３】

図３



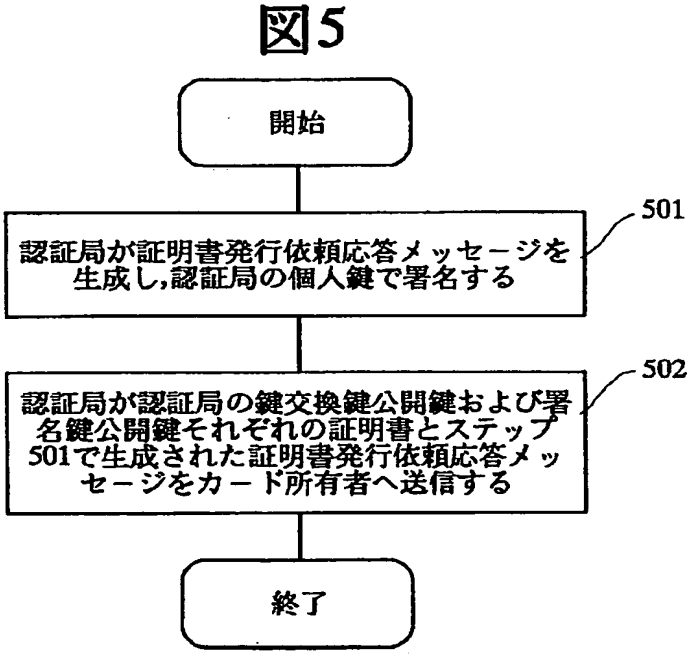
【図２】

図２


10
認証局サーバ
110
114
キーボード
113
表示器
112
通信装置
制御装置
111
記憶装置
115
11511
署名鍵公開鍵PBCPS0
署名鍵個人鍵PVCPS0
11512
11513
証明書
CertPBCPS0
11510
30
120
123
通信装置
122
通信装置
124
表示器
制御装置
121
キーボード
125
記憶装置
126
12610
Ｗｅｂサーバ
ソフトウエア
認証局Webサーバ
11521
鍵交換鍵公開鍵PBCPEX
鍵交換鍵個人鍵PVCPSEX
11522
11523
証明書
CertPBEX
11520
11531
11532
11533
ブランド名
証明書
証明書名組
a
C5
C2∧C3
B
C4
(C1∧C2)∨C3
11530
11541
11542
11543
証明書
対象
公開鍵
C4
A
PkA
C3
B
PkB
11540

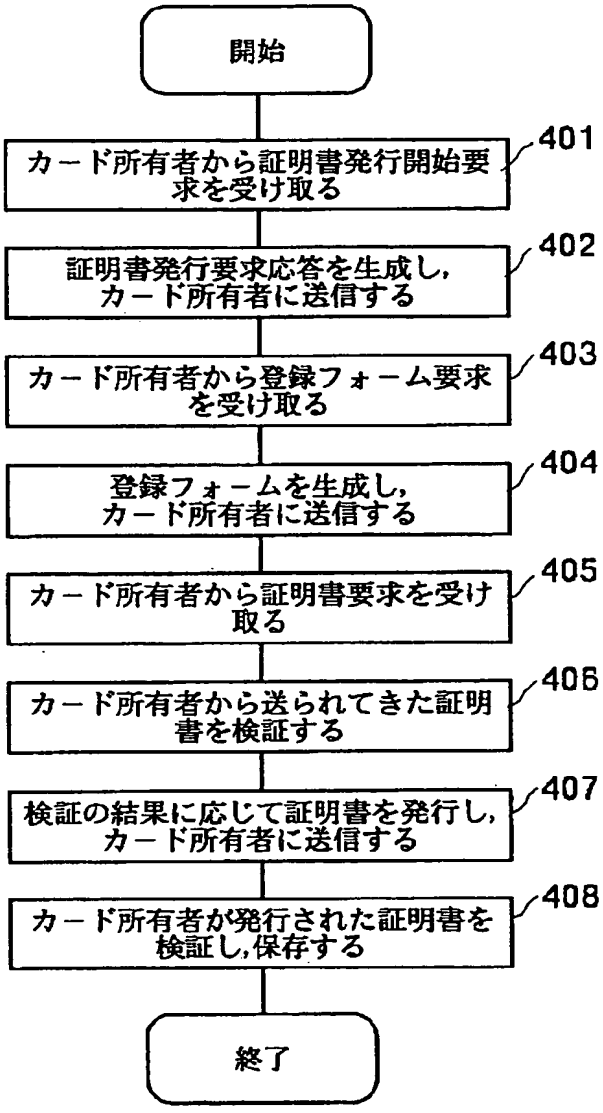
【図５】

図５


開始
認証局が証明書発行依頼応答メッセージを生成し,認証局の個人鍵で署名する
501
認証局が認証局の鍵交換鍵公開鍵および署名鍵公開鍵それぞれの証明書とステップ501で生成された証明書発行依頼応答メッセージをカード所有者へ送信する
502
終了

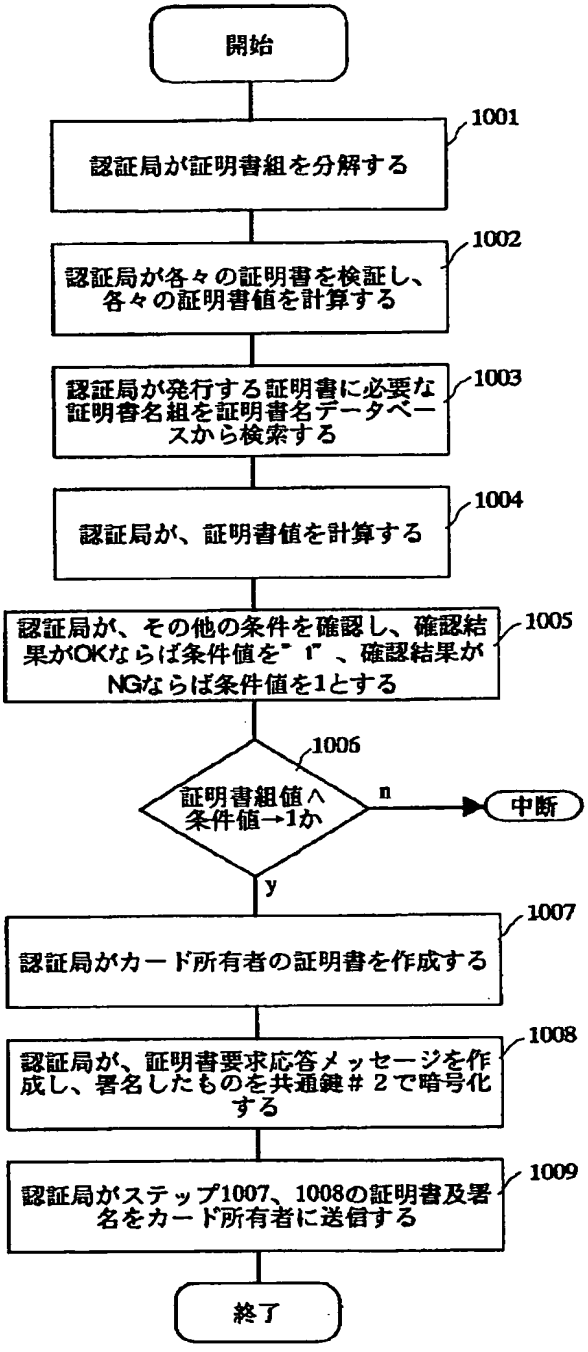
【図４】

図4


開始
カード所有者から証明書発行開始要求を受け取る
401
証明書発行要求応答を生成し，カード所有者に送信する
402
カード所有者から登録フォーム要求を受け取る
403
登録フォームを生成し，カード所有者に送信する
404
カード所有者から証明書要求を受け取る
405
カード所有者から送られてきた証明書を検証する
406
検証の結果に応じて証明書を発行し，カード所有者に送信する
407
カード所有者が発行された証明書を検証し，保存する
408
終了

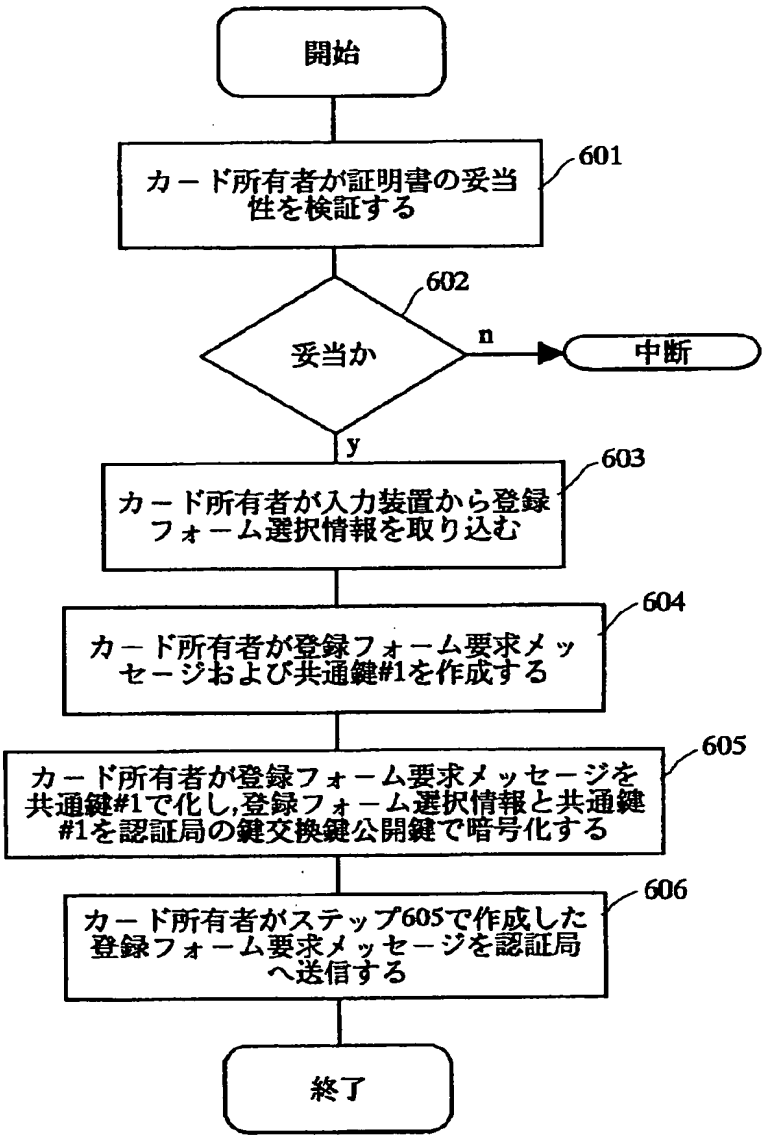
【図１０】

図10


開始
認証局が証明書組を分解する
1001
認証局が各々の証明書を検証し、各々の証明書値を計算する
1002
認証局が発行する証明書に必要な証明書名組を証明書名データベースから検索する
1003
認証局が、証明書値を計算する
1004
認証局が、その他の条件を確認し、確認結果がOKならば条件値を" r" 、確認結果がNGならば条件値を1とする
1005
証明書組値∧条件値→1か
1006
n
中断
y
認証局がカード所有者の証明書を作成する
1007
認証局が、証明書要求応答メッセージを作成し、署名したものを共通鍵＃２で暗号化する
1008
認証局がステップ1007、1008の証明書及署名をカード所有者に送信する
1009
終了

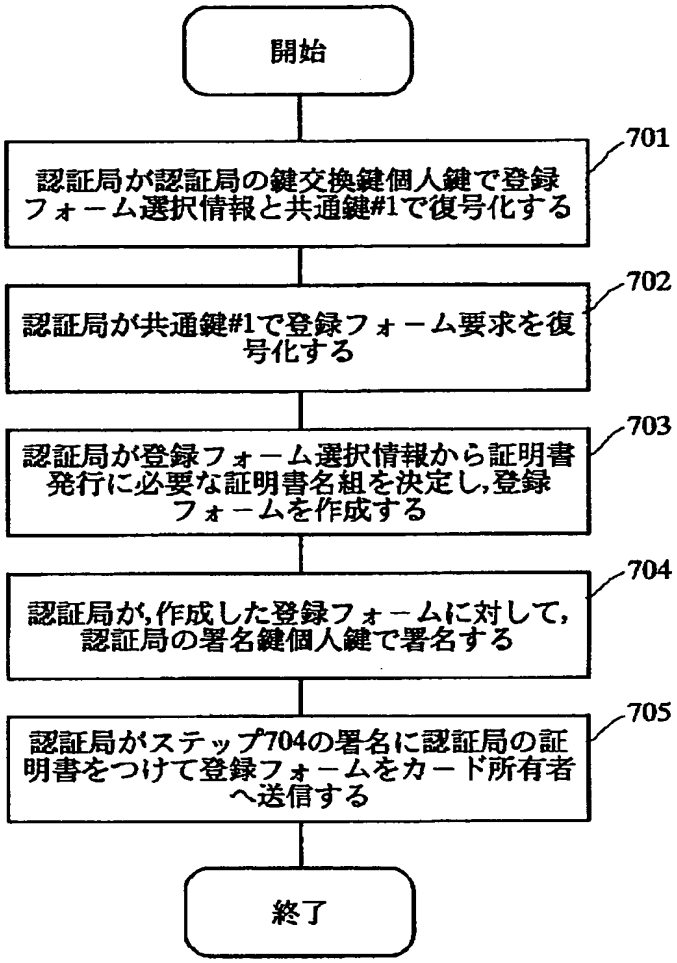
【図６】

図6


開始
カード所有者が証明書の妥当性を検証する
601
602
妥当か
n
中断
y
カード所有者が入力装置から登録フォーム選択情報を取り込む
603
カード所有者が登録フォーム要求メッセージおよび共通鍵#1を作成する
604
カード所有者が登録フォーム要求メッセージを共通鍵#1で化し,登録フォーム選択情報と共通鍵#1を認証局の鍵交換鍵公開鍵で暗号化する
605
カード所有者がステップ605で作成した登録フォーム要求メッセージを認証局へ送信する
606
終了

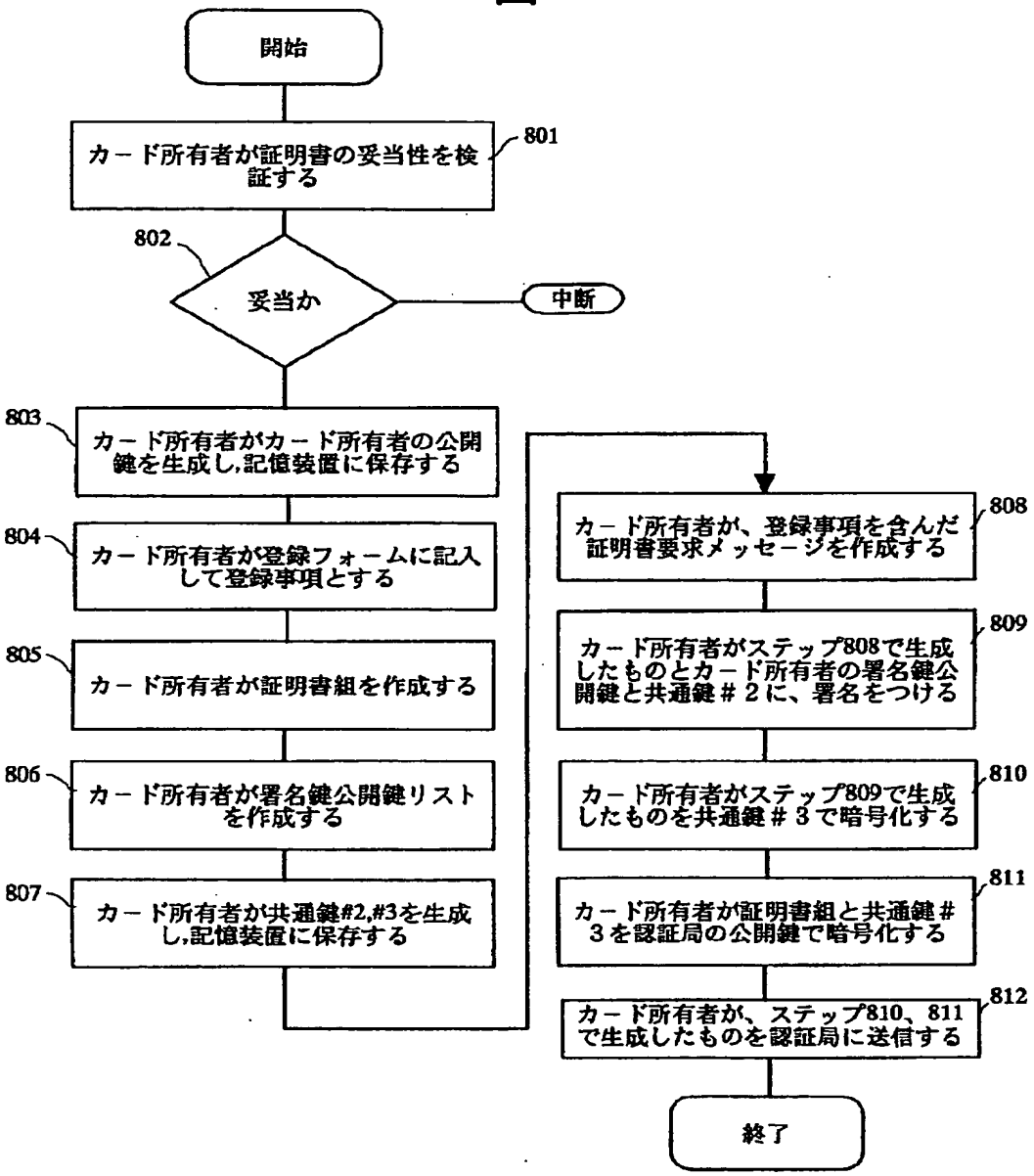
【図７】

図7


開始
認証局が認証局の鍵交換鍵個人鍵で登録フォーム選択情報と共通鍵#1で復号化する
701
認証局が共通鍵#1で登録フォーム要求を復号化する
702
認証局が登録フォーム選択情報から証明書発行に必要な証明書名組を決定し,登録フォームを作成する
703
認証局が,作成した登録フォームに対して,認証局の署名鍵個人鍵で署名する
704
認証局がステップ704の署名に認証局の証明書をつけて登録フォームをカード所有者へ送信する
705
終了

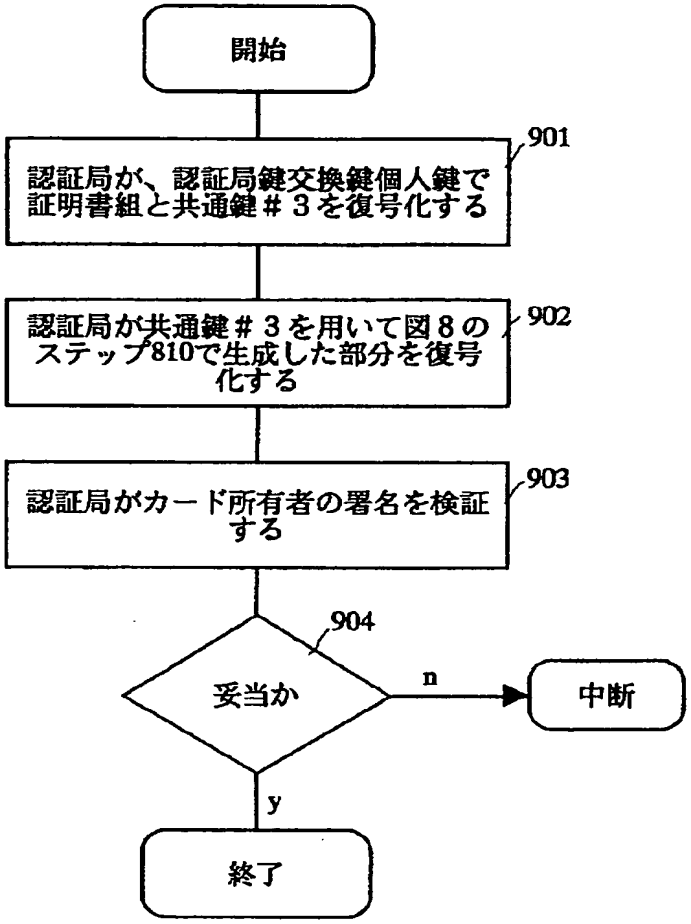
【図８】

図8


開始
カード所有者が証明書の妥当性を検証する
801
802
妥当か
中断
803
カード所有者がカード所有者の公開鍵を生成し,記憶装置に保存する
804
カード所有者が登録フォームに記入して登録事項とする
805
カード所有者が証明書組を作成する
806
カード所有者が署名鍵公開鍵リストを作成する
807
カード所有者が共通鍵#2,#3を生成し,記憶装置に保存する
808
カード所有者が、登録事項を含んだ証明書要求メッセージを作成する
809
カード所有者がステップ808で生成したものとカード所有者の署名鍵公開鍵と共通鍵＃２に、署名をつける
810
カード所有者がステップ809で生成したものを共通鍵＃３で暗号化する
811
カード所有者が証明書組と共通鍵＃３を認証局の公開鍵で暗号化する
812
カード所有者が、ステップ810、811で生成したものを認証局に送信する
終了

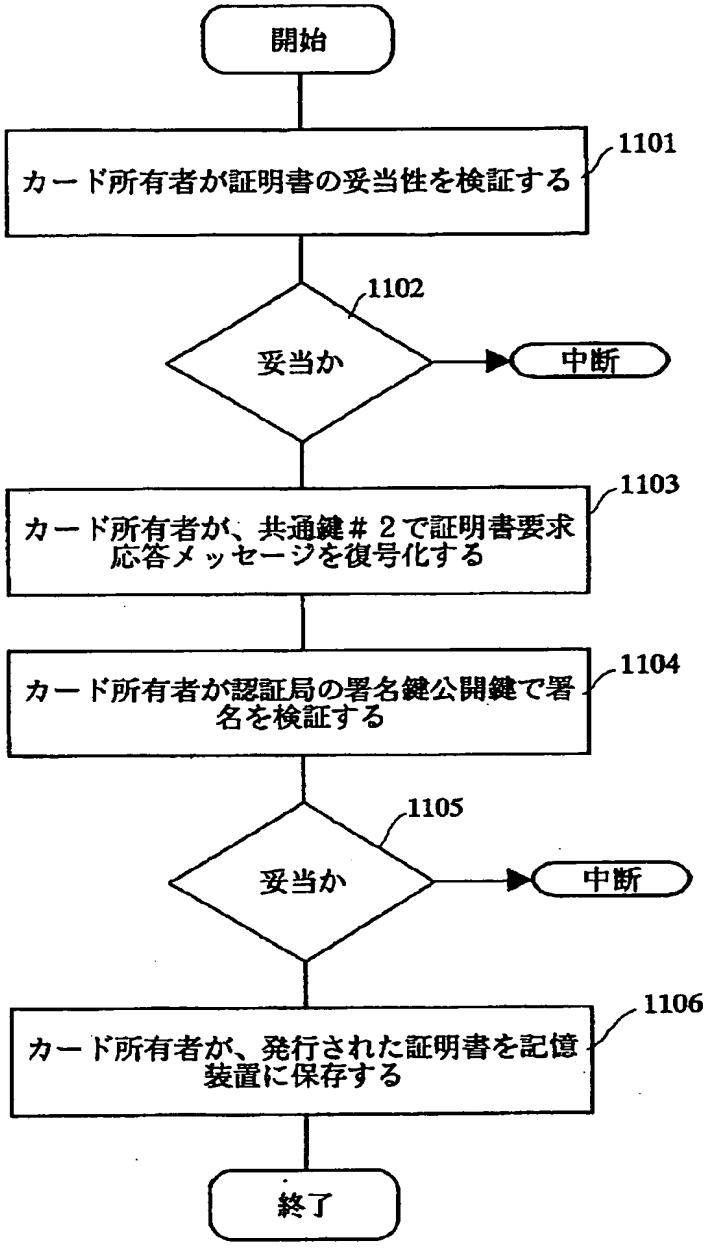
【図９】

図９


開始
901
認証局が、認証局鍵交換鍵個人鍵で証明書組と共通鍵＃３を復号化する
902
認証局が共通鍵＃３を用いて図８のステップ810で生成した部分を復号化する
903
認証局がカード所有者の署名を検証する
904
妥当か
n
中断
y
終了

【図１１】

図１１



フロントページの続き

(72)発明者 川連 嘉晃
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内

(72)発明者 松永 和男
神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内

(72)発明者　州崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内